# Patent Application Cover Page

# FILTERED EMAIL DIFFERENTIATION

Inventor:

**Daniell, William T.**

Jeffrey R. Kuester
Charles W. Griggers
Thomas, Kayden, Horstemeyer & Risley LLP
100 Galleria Parkway
Suite 1750
Atlanta, GA 30339
Tel: 770.933.9500
Fax: 770.951.0933

Attorney Ref. No.: 190250-1570
BellSouth Ref. No.: BLS-030454

Customer No.: 38823

# FILTERED EMAIL DIFFERENTIATION

## CROSS-REFERENCE TO RELATED APPLICATION

[0001] This application is related to copending U.S. utility patent application entitled "Consolidated Email Filtering User Interface" filed on the same day as the present application and accorded serial number *[xx/xxx,xxx]*, which is entirely incorporated herein by reference.

## TECHNICAL FIELD

[0002] The present disclosure relates generally to digital communication and, more particularly, to email.

## BACKGROUND

[0003] With the advent of the Internet, email has become prevalent in digital communications. For example, email messages are exchanged on a daily basis to conduct business, to maintain personal contacts, to send and receive files, *etc.* Unfortunately, undesired email messages have also become prevalent with increased email traffic. Often, these email messages are unsolicited advertisements, which are often referred to as "junk mail" or "spam." Currently, software applications exist, which remove some of the spam or junk mail from a recipient's email account (or mailbox), thereby reducing clutter in the recipient's email account. Email messages that are determined to be spam or junk mail are either removed (*e.g.*, permanently deleted) or stored in a designated folder (*e.g.*, "trash" folder, "junk mail" folder, "spam" folder, *etc.*). Such applications, however, still may not be adequate to effectively remove undesired email messages.

[0004] Thus, a heretofore unaddressed need exists in the industry to address the aforementioned deficiencies and inadequacies.

## SUMMARY

[0005] The present disclosure provides for removing undesired email messages. In this regard, some embodiments, among others, comprise providing a plurality of detection mechanisms for detecting undesired email messages. Accordingly, a user interface is provided to display an identification of an undesired email message in a particular visual manner that is associated with a particular detection mechanism.

[0006] Systems, methods, features, and advantages will be or become apparent to one with skill in the art upon examination of the following drawings and detailed description.

## BRIEF DESCRIPTION OF THE DRAWINGS

[0007] Many aspects of the disclosure can be better understood with reference to the following drawings. The components in the drawings are not necessarily to scale, emphasis instead being placed upon clearly illustrating the principles of the present disclosure. Moreover, in the drawings, like reference numerals designate corresponding parts throughout the several views.

[0008] FIG. 1 is a block diagram of one embodiment of the detection management system.

[0009] FIG. 2 is a block diagram of one embodiment of an email application for the detection management system of FIG. 1.

[0010] FIG. 3 is a diagram showing one embodiment of a message center for the user interface logic of FIG. 2.

[0011] FIG. 4 is a diagram showing one embodiment for managing one or more spam detection schemes with the user interface logic of FIG. 2.

[0012] FIG. 5 is a diagram showing one embodiment for editing an allow list with the user interface logic of FIG. 2.

[0013] FIG. 6 is a diagram showing one embodiment editing a block lost with the user interface logic of FIG. 2.

[0014] FIG. 7 is a diagram showing one embodiment for adding an objectionable word or phrase to an objectionable word and phrase list with the user interface logic of FIG. 2.

[0015] FIG. 8 is a diagram showing one embodiment of the message center for the user interface logic of FIG. 2.

[0016] FIG. 9A is a diagram showing one embodiment of a read window for the user interface logic of FIG. 2.

[0017] FIG. 9B is a diagram showing one embodiment of a read window for the user interface logic of FIG. 2.

[0018] FIG. 10 is a diagram showing one embodiment of a user interface for adding the sender of the particular message to a block list of FIG. 6.

[0019] FIG. 11 is a flowchart showing one embodiment of a method for managing spam detection schemes of an email application of FIG. 1.

[0020] FIG. 12 is a flowchart showing one embodiment of a method for visually representing a spam message according to a particular spam detection scheme of FIG. 4.

[0021] FIG. 13 is a flowchart showing one embodiment of a method for detecting an undesired email message using a plurality of spam detection schemes.

## DETAILED DESCRIPTION

[0022] Reference is now made in detail to the description of the embodiments as illustrated in the drawings. While several embodiments are described in connection with these drawings, there is no intent to limit to the embodiment or embodiments disclosed herein. On the contrary, the intent is to cover all alternatives, modifications, and equivalents.

[0023] The present disclosure provides communication systems and methods for managing the detection of undesired email messages. FIG. 1 is a block diagram of one embodiment of the detection management system 100. As shown in FIG. 1, the detection management system 100 comprises representative workstations 102, 104, 106 that are coupled to a server 110 over a network such as the Internet 120. The server 110 is coupled to a database 115 that stores email accounts (or mailboxes) of various users.

[0024] In the operating environment shown in FIG. 1, a sender of an email message generates the email message at a sender workstation 102 and sends the email message through a network 120 (via the server 110 and database 115) to a recipient at a recipient workstation 106. As shown in FIG. 1, the recipient workstation 106 includes a processor 152, a network interface 160, memory 154, a local storage device 158, and a bus 156 that permits communication between the various components. While not explicitly shown, it should be appreciated that the other workstations 102, 104 may also include similar components that facilitate computation or execution of applications on the workstations 102, 104. In some embodiments, the local storage device 158 may be a hard drive configured to electronically store data. The local storage device 158 may also store computer programs that execute on the recipient workstation 106. In this sense, the processor 152 is preferably configured to access any program that is stored on the local storage device 158, and execute the program with the assistance of the memory 154. In the embodiment of FIG. 1, an email application 155 is shown as being loaded into memory 154 for launching at the workstation 106, thereby permitting the workstations 106 to send and receive email messages through the network 120. Since the functioning

of computing devices is well known in the art, further discussion of the processor 152, memory 154, and the local storage device 158 are omitted here. However, it should be appreciated that the memory 154 may preferably be either volatile or non-volatile memory.

[0025] The network interface 160 is configured to provide an interface between the recipient workstation 106 and the network 120. Thus, the network interface 160 provides the interface for the workstation 106 to receive any data that may be entering from the network 120 and, also, to transmit any data from the workstation 106 to the network 120. Specifically, in some embodiments, the network interface 160 is configured to permit communication between each of the workstations 102, 104, 106 and the server 110 and, additionally, to permit communication between the workstations 102, 104, 106 themselves. In this regard, the network interface 160 may be a modem, a network card, or any other interface that communicatively couples each of the workstations 102, 104, 106 to the network. Since various network interfaces are known in the art, further discussion of these components is omitted here. It should be understood that various aspects of the email application 155 may be conventional or may be custom tailored to specific needs.

[0026] Referring now to FIG. 2, shown is a more detailed diagram of the email application 155 of FIG. 1. The email application preferably includes POP3 and SMTP components 210. As one skilled in the art will recognize, these protocols merely relate as examples to retrieving and sending email messages. As such, it is intended that other protocols and architectures that operate to send and retrieve email messages, such as IMAP4, among others, are intended to be included herein. For example, other alternative embodiments of the email application 155 include components for downloading of email messages that have been stored in a server 110 for a workstation 106 that has LAN or Web access.

[0027] The POP3 component 210 in this embodiment typically downloads email messages from the server 110 through the network interface 160, and stores the email messages in non-volatile storage which may be referred to as a mail store 220. A rules engine 230 sorts and filters the email messages according to specified rules before the email messages are deposited in the mail store 220. For example, one rule may stipulate that each email message should be examined to determine if the message is "spam," and another rule may specify that any message from a certain sender should be automatically

deleted, *etc*. Note, the POP3 server in this embodiment can be set up to retrieve messages for more than one email account. Further, the term "spam" is being used to generally refer to any undesired email message that may be sent to a user, including unsolicited email messages, offensive email messages, *etc*., among others. Accordingly, spam messages may be sent from commercial and non-commercial senders.

[0028] User interface logic 240 included within the email application 155 can retrieve the messages from the mail store 220, format the information, and send the formatted information to the I/O display device 150. In particular, user interface logic 240 of this embodiment, among others, of the present invention is configured to parse the data retrieved from mail store 220. Specifically, user interface logic 240 can separate email messages according to an associated "To:" email address or "From:" email address, and display multiple mailboxes corresponding to several email addresses. User interface logic 240 is also preferably configured to display identification and summary information from each of the mailboxes, such as sender name and subject identification, as well as a summary of how many messages are contained in each of the subfolders of the mailboxes, among others. One skilled in the art will recognize that in practice, user interface logic 240 typically calls various functions within the operating system that are relayed through the processor 152 before being sent to the display device 150.

[0029] FIG. 3 is a screen diagram display representing one embodiment of a message center 300 for the user interface logic 240 of FIG. 2. As shown in FIG. 3, the message center 300 for the user interface logic 240 comprises a send or receive selection button 310, a write selection button 315, a mail options selection button 320, an address book database selection button 325, a spam controls selection button 330, and a folder options selection button 335. For example, if a user selects the address book database selection button 325, then an address book user interface (not shown) is launched or instantiated as is commonly understood in the art. If the user selects the write selection button 315, then a compose window (not shown) is launched or instantiated as is commonly understood in the art. Similarly, if the user selects the send or receive selection button 310, then any prepared messages are sent and the designated mail servers for the user are checked for new mail, as is commonly understood in the art.

[0030] In addition to the selection buttons 310, 315, 320, 325, 330, 335 the message center 300 includes a display screen 345, which displays identifications 346 of received email messages in an identification panel 347 and preferably displays a preview pane 350

having a preview of a selected email message for an active persona (*e.g*, Joe, Sr., as opposed to Joe Jr., as shown). The display screen 345 also includes message response options 348 such as replying to the email message, forwarding the email message, reading the full email message (rather than merely previewing the email message in the preview pane), deleting the email message, or printing the email message. For example, if the user selects the read selection button 349, then a read window (not shown) is launched or instantiated as is commonly understood in the art. As known to those skilled in the art, there are many different ways to facilitate reading and writing a message, and the invention presented herein should not be limited to a particular method for displaying the text of a message or for composing a message.

[0031] The message center 300 also includes a folder list 305 having a plurality of folders which have various email messages that may be organized according to message type, such as an inbox folders 305a, spam folder 305b, drafts folder 305c, outbox folder 305d, saved items folder 305e, trash folder 305f, *etc*. The message center 300 currently shows, for example, a folder list for Joe Sr. 305 and a folder list for his adolescent son, Joe Jr. 306. Note, the folder list of Joe. Jr. preferably does not have a spam folder. Accordingly, in some embodiments, spam messages that are intended for Joe. Jr. are automatically placed in the spam folder 305b of another user, such as a parent Joe. Sr. This operation is discussed later in reference to tag identifiers for spam messages.

[0032] Referring again to FIG. 3, upon selecting the folder options selection button 335, the user may configure and store unique folder options specifically for that user. In a similar manner, selection of the mail options selection button 320 may also provide customized mail settings (*e.g*., mail delivery rates) that may be customized according to different groupings of communications accounts and/or services. Similarly, if the user selects the spam controls selection button 330, then a user spam controls window (not shown) for configuring spam settings is launched or instantiated. The spam controls window preferably enables a user to effectively manage various spam detection schemes in a consolidated manner, as discussed below.

[0033] FIG. 4 is a diagram showing one embodiment of a user interface 400 for managing a plurality of spam detection schemes. As shown in FIG. 4, the user interface 400 comprises a radio-style selection button 410 to indicate if a user has activated spam filtering for email messages that are to be delivered to the user's inbox. Preferably, if enabled, spam detection mechanisms attempt to detect and filter out undesired email

messages from incoming email messages before the email messages reach a user's inbox. The undesired email messages are typically stored in a user's spam folder 305b. In some embodiments, the rules engine 230 of FIG. 2 employs a variety of spam detection mechanisms. To wit, the rules engine 230 preferably executes rules that are intended to detect undesired email messages or spam. For example, the rules engine 230 may perform rules that attempt to recognize certain features that are prevalent in spam messages. Further, the rules engine 230 may perform rules that implement a statistical algorithm, such as a Bayesian-type, to determine if an incoming message may be spam, based upon the overall similarity between the incoming message and previous spam messages.

[0034] Accordingly in FIG. 4, the user interface 400 provides a sliding scale representation 420 whereby a user can specify the level of overall likelihood of spam (sensitivity of filtering) that is utilized in a statistical filtering algorithm. If the scale is positioned to the far left, than an incoming message that has a low level of similarity with previous spam messages will be determined to be spam. Accordingly, as the scale is moved to the right, the level of similarity is gradually increased, and thus, an incoming email message has to have a higher level of similarity with previous spam messages to be determined to be, and filtered out as, spam.

[0035] The user interface 405 further comprises radio-style selection buttons 430 that may be selected to activate/deactivate a mechanism for removing incoming messages that are from unauthorized senders. For example, a user may select the top selection button to indicate that an incoming email message that is not from an authorized list of senders should be designated as spam and stored in the spam folder for the user ("Joe Sr.") 305b. Accordingly, the user may select the edit allow list selection button 440 to add and remove senders from the "allow list," as shown below.

[0036] FIG. 5 is a diagram showing one embodiment 500 of a user interface for adding senders to, and removing senders from, the "allow list." To add a sender, the user may enter a complete email address or a domain name into the input box 515 and select the add selection button 520. Accordingly, the entered name will be added to the list of email addresses and domain names that make up the "allow list" 530. Further, a user may remove an email address or domain name that is on the allow list 530 by selecting the address/name (*e.g.*, by highlighting the address/name) and selecting the remove button 540.

[0037] Referring back to FIG. 4, instead of authorizing senders from an allow list, a user may select the bottom radio-style selection button 430 to indicate that an incoming email message that is from a list of unauthorized senders should be designated as spam and stored in the spam folder for the user 305b. Accordingly, the user may select the edit block list selection 445 button to add and remove senders from the "block list," as shown below.

[0038] FIG. 6 is a diagram showing one embodiment 610 of a user interface for adding senders to, and removing senders from, the "block list." To add a sender, the user may enter a complete email address or a domain name into the input box 615 and select the add selection button 620. Accordingly, the entered name will be added to the list of email addresses and domain names that make up the "block list" 630. Further, a user may remove an email address or domain name that is on the block list 630 by selecting the address/name (*e.g.*, by highlighting the address/name) and selecting the remove button 640.

[0039] Referring back to FIG. 4, the user interface 400 further comprises radio-style selection buttons 450 to activate/deactivate a text filtering mechanism. For example, a user may select the top selection button 450 to indicate that the textual content of an incoming email message should be checked against a list of offensive words and phrases. If an incoming email message is determined to contain a word or phrase that has been deemed offensive, than the email message is stored in a spam folder 305b. Typically, the list of objectionable words and phrases has been pre-compiled and does not have to be created by the user. However, a user may modify the list by adding or removing words or phrases from the list. For example, to add an offensive word or phrase to the objectionable word/phrase list, a user may select the edit text filter button 460, as shown below.

[0040] FIG. 7 is a diagram showing one embodiment 700 of a user interface for adding an objectionable word or phrase to the objectionable word and phrase list. To add a word or phrase, the user may enter the word or phrase into the input box 715 and select the add selection button 720. Accordingly, the entered word or phrase will be added to the list of objectionable words and phrases. An alternative mechanism for adding or removing a word or phrase to the objectionable word and phrase list may be associated with the spam folder 305b and is discussed later in reference to FIG. 9A.

[0041] Referring again to FIG. 4, after a user has provided selections for each of the

spam filtering techniques, the user may confirm his or her selections by selecting the OK button 470. Otherwise, the user may nullify his or her selections by selecting the cancel button 475. In other embodiments, different spam detection schemes may also be employed on a single graphical control or window interface. For example, another type of spam detection mechanism, not previously mentioned, allows messages from designated senders who have been specified on a particular list of senders by the user and then allows messages from senders who are not on the particular list to be processed by other spam detection schemes. In this way, the user is able to still receive messages from senders that are not on the particular list, as long as the messages are not designated as spam by another spam detection mechanism. In some embodiments, among others, the particular list of senders provided by the user is the user's address book of email addresses. Further, some embodiments verify that a sender (who is in the user's address book) of a received email message is legitimate by performing a Domain Name Server (DNS) look-up of the domain name of the Simple Mail Transfer Protocol (SMTP) server (using the originating IP address in the received email message header) that was used to originally send the email message. Then, the domain name of the SMTP server is compared to the listed domain name of the sender in the From: field of the email message to insure that the domain name of the actual sender of the email message is the same as the listed domain name in the From: field.

[0042] Accordingly, in some embodiments, among others, a user may specify various combinations of spam detection schemes to provide varying security levels of spam protection. For example, in the embodiment shown in FIG. 4, spam detection schemes involving a statistical filtering algorithm 420 and a block list 430 have been activated, while a spam detection scheme involving an allow list 430 and text filtering 450 has not been activated. Next, some techniques for modifying particular spam detection scheme settings are discussed below.

[0043] FIG. 8 is a diagram showing one embodiment of the message center 312 for the user interface logic 240 when the spam folder 305b has been selected for viewing. In this regard, once the spam folder 305b has been selected, identifications 825 of the email messages contained in the spam folder 305b are presented to the user. As shown in FIG. 8, the spam folder 305a, which belongs to Joe Sr., contains email messages from C. Caustic, spam.com, J. Smith, and junk.com. For spam folder 305b, the feature of displaying a preview of a selected message has been disabled in some embodiments, since

the contents in a spam folder has been determined to be objectionable or undesired. Hence, in the example of FIG. 8, if J. Smith's email message is selected, then the contents of that email message may not be displayed in the preview window 350 below the list of email messages. Further, when the spam folder has been selected for viewing, the mark as spam button 390 of FIG. 3 is disabled and/or hidden, since the messages in the spam folder 305b have already been marked as spam. However, a message in a spam folder 305b may be viewed by using the message center 300 to select a message from the spam folder 305a and then selecting the read button 349. A read window will then open, enabling the user to read the text associated with the selected message, as discussed below.

[0044] FIG. 9A is a diagram showing one embodiment of a read window 900 for user interface logic 240 when a message from a spam folder 305b has been selected. As shown in FIG. 9A, one embodiment of the read window 900 comprises several selection options that a user may select. For example, a user may select an email reply button 902, an email forward button 904, a print button 906, and a delete button 908 from the email read window 900. Since these functions are well known in the art, further discussion of email reply, email forward, print, and delete functions are omitted here. However, it is worthwhile to note that, unlike prior systems, the selection of the unmark as spam button 910, in some embodiments, permits the user to move a message that has been marked as a spam message and stored in the spam folder 305b to the inbox folder 305a of the user (Joe, Sr.).

[0045] Correspondingly, as shown in FIG. 3, the selection of a non-designated spam folder (*e.g*, inbox folder) allows the user to select the mark as spam button 390 to move a message in the non-designated folder to the spam folder and to have the message marked and designated as spam. Once a message has been manually marked as spam by the user, the user may also be presented with a user interface 1000 for adding the sender of the particular message to the block list, as shown in FIG. 10. By selecting the yes button 1010, the full email address of the sender is added to the block list 630.

[0046] Of further note, within the text of a message that has been marked as spam, the words or phrases that were detected by the text filtering mechanism may be highlighted 920, as shown. Moreover, in some embodiments of the user interface 900, a user may use a mouse or keyboard to perform a "right click" operation to select a remove from list option 930 to indicate that the user would like the highlighted word/phrase to be

removed from the list of objectionable words and phrases, as shown in FIG. 9A. Correspondingly, a user may select a word that has not been highlighted within the text of the message and may manually highlight the word or phrase. Then, the user may perform a "right click" operation on the word or phrase and select an "add to list" option (not shown) to indicate that the word or phrase should be added to the list of objectionable words and phrases. Accordingly, this operation may be performed with regard to messages in other folders besides the spam folder 305b.

[0047] As discussed above, certain incoming email messages may be stored in the spam folder 305b. Thus, when the user (Joe Sr., in the example of FIG. 3) selects the spam folder 305b, then a list 825 of spam email message identifications is displayed to the user. Note, each email message that is stored in the spam folder 305b is preferably embedded with an indicator (*e.g*, a particular tag, marker, *etc.*) that shows that the message has been designated as a spam message. Further, each email message in the spam folder 305b is preferably identified with a separate indicator for each of a variety of spam detection schemes. For example, if the email messages from both J. Smith and C. Caustic were determined to be spam or undesired email messages because each email message contains words or phrases in the list of objectionable words and phrases, then the email messages from J. Smith and C. Caustic may contain a first indicator associated with a text-filtering detection scheme. Alternatively, if the email message from spam.com was determined to be spam because the spam.com domain name is on the block list of the user, then the email message from spam.com may have a second indicator associated with a block list detection scheme. Accordingly, additional indicators may be associated with other spam detection schemes. For example, various other spam detection schemes include spam filters based on various methodologies or algorithms, manual detection by a user, *etc.*

[0048] Further, each identification of an email message that is marked by a particular indicator may be displayed in a particular manner within the spam folder 305a by the message center 300 (*e.g.*, displayed with a particular font, style, color, *etc.*). For example, an identification of spam message that contains a first indicator may be displayed with italic lettering, as shown in FIG. 8. Alternatively in some embodiments, for example, identification of a spam message that contains a first indicator may be displayed in a particular color, while identification of a spam message embedded with a different indicator maybe displayed in a different color. For example, a spam email identification

displayed in a blue color may be associated with a block list detection scheme. Hence, by viewing the appearance of an identification of a spam message, a user may determine the type of spam detection scheme that designated the message as spam and caused the message to be placed in the spam folder 305b. Other embodiments include appearance modifications for email messages themselves. Therefore, if the user discovers that a "desired" message was placed in the spam folder, the user can readily determine which particular detection scheme designated the message as spam. Accordingly, the user may alter the settings or parameters of the particular detection scheme to prevent a similar situation from reoccurring. For example, if a particular message was designated to be spam, the user may ascertain from the look or appearance of the identification of the message (*e.g.*, displayed in an orange color) that the message was deemed to be spam because of the message contained a certain word that was in the objectionable word list of a text-filtering detection scheme. Therefore, the user may remove the word from the list, as discussed in reference to FIG. 9A.

[0049] A user in some embodiments may drag identifications of email messages between the user's inbox folder 305a and spam folder 305b in either direction (*e.g.*, via a drag and drop operation). Accordingly, the drag and drop operation of moving a message identification from a spam folder 305b to the inbox folder 305a automatically removes the indicator of a particular detection scheme that previously marked the message as a spam message. Further, the user may be prompted to update or adjust the settings or preferences of the particular detection mechanism after the drag and drop operation.

[0050] For example, the rules engine 230 may place a particular email message in a user's spam folder 305b because the sender of the particular email message was on the user's block list 630. However, the user may later drag the email message identification from the spam folder 305b to the inbox folder 305a. Accordingly, user interface logic 240, upon detecting the drag and drop operation, may activate a mechanism for prompting the user to adjust settings for the particular detection scheme that was associated with the particular email message. For example, if the particular email message was previously marked with an indicator of the block list detection scheme, the user may be prompted to remove the sender from the user's block list 630. Alternatively, if the particular email message was previously marked with an indicator for the text-filtering detection scheme, the user may be prompted to remove the word or phrase that caused the email message to be marked as spam from the list of objectionable words and

phrases, for example. Correspondingly, after the email message has been removed from the spam folder 305b, the current content of all the email messages in the spam folder 305b may then be re-examined according to a statistical alogrithm, such as a Baysesian-type, since the content of the spam folder 305b has changed.

[0051] In the inverse operation of dragging an email message identification from the inbox 305a to the spam folder 305b, the contents of the spam folder 305b, after the email message has been removed from the inbox and added to the spam folder 305a, are also examined under a statistical algorithm, such as a Bayesian-type. Accordingly, user interface logic 240 upon detecting the drag and drop operation may activate a mechanism for prompting the user to mark the email message as a certain type of spam using an indicator associated with one of the particular detection scheme mechanisms.

[0052] For example, if a user moves a particular email message from the inbox 305a to the spam folder 305b because of a particular objectionable word in the particular email message, the user may be prompted to specify that the particular email message has been determined to be spam because of an objectionable word or phrase. Accordingly, the email message may be marked with an indicator for the text-filtering detection scheme (that detects objectionable words and phrases).

[0053] Further, upon selection of a particular type of spam, the user may be prompted to adjust the settings associated with the particular spam detection scheme that detects that particular type of spam. Accordingly, in the present case, the user may prompted to add the particular objectionable word to the list of objectionable words and phrases utilized by the text-filtering detection scheme. Alternatively, for other types of spam, the user may prompted to adjust other settings, such as adding a sender of an email message to the user's block list 630.

[0054] Typically, the format of an email message contains markers or tags (*e.g.*, to: tag, cc: tag, *etc.*) to instruct an email application 155 on how the message should appear on a display device 150 when shown. Accordingly, in some embodiments of the invention, special tag or marker indicators are placed within the format of the respective email messages to identify an email message as a spam message. Further, special tag indicators are also placed within the format of respective email messages to indicate that the message was detected by a particular spam detection scheme. Referring back to FIG. 2, the rules engine 230 may perform a rule designed to detect an incoming spam message. Further, the rules engine 230 may perform more than one rule that is directed toward

detecting spam messages. For example, one rule may implement a Bayesian filtering approach and another rule may implement a text-filtering approach, for example.

[0055] Accordingly, if a particular spam message is detected by the rules engine 230, then the rules engine 230 may be configured to insert a special marker or tag identifier into the format of the particular spam message to indicate it as such (*i.e.*, a particular spam message). In addition, user interface logic 240 may be directed to insert a special marker or identifier tag into the format of an email message that the user wants to manually designate as a spam message, as discussed previously. Therefore, the user interface logic 240 can later recognize that the message is spam by recognizing the special identifier tag in its formatting. Extensible markup language (XML) is one language, among others, that may be used to describe the contents of an email message by using markers or tags, according to the previously described embodiments.

[0056] Note, the user interface logic 240 may also perform particular operations that are associated with a particular marker or tag identifier contained in an email message. For example, in some embodiments, a read window may show an email message that has a tag identifier associated with a text-filtering detection scheme and highlight the words within the message that are contained on a list of objectionable words and phrases. However, this operation may not be performed for spam messages detected by other detection schemes and associated with other tag identifiers.

[0057] In addition, a spam message that is intended for a user who has been classified as a "child" may be stored in spam folder of a parent or some other designated user. For example, a message intended for a child may be marked with a tag or marker that indicates that the intended recipient is a "child." Accordingly, the same message may be marked by an identifier that designates the message as spam. Therefore, a particular operation may be performed for messages that contain both the child tag and the spam identifier. To wit, user interface logic 240 may be configured to detect the "child" marker and the "spam" marker in message and upon detection, perform the operation of moving the message to the spam folder of another user, such as a parent of a the user. Correspondingly, a user interface of the other user ("adult") may represent the spam messages of the child in a different manner than spam messages of the adult, since both types of messages may be stored in a single spam folder of the adult.

[0058] As shown in FIG. 9B, alternative embodiments of the user interface 900 may

provide a button 940 to activate a mechanism 950 for displaying a list of the particular objectionable words and phrases that are contained within a particular email message and how many instances each objectionable word or phrase occurred. By clicking on the particular word or phrase in the list, a user may advance to the particular instance in the message to review the word and surrounding text. Further, the user may directly remove, replace, or skip (allow once) the instance of the usage of the particular word or phrase in the message via the mechanism 950. In this manner, the user may clean up and sanitize the email message. For example, to replace a word or phrase, a mechanism 960 for substituting a word may be activated from the mechanism 950 for displaying a list. Accordingly, the mechanism 960 for substituting a word presents alternative words that can be substituted for the objectionable word or phrase.

[0059] Consider, an email message that is intended for a child and has been determined to be spam by the rules engine 230. If the email message was detected by a text-filtering mechanism, the email message may be cleaned by an adult user, for example. In some embodiments, after the email message has been reviewed and sanitized according to the adult user's level of satisfaction, the adult user may drag and drop the email message to the child's inbox folder. In other embodiments where the email message is located in the adult user's spam folder 305b, after the email message has been reviewed and sanitized according to the adult user's level of satisfaction, the adult user may unmark the email message as spam which causes the message to automatically move to the child's inbox.

[0060] Having described several embodiments of systems for effectively managing various spam detection schemes in a consolidated manner, attention is turned to FIGs. 11-12 which show several embodiments of methods for managing spam detection schemes. FIG. 11 is a flowchart showing an embodiment of a method for managing spam detection schemes of an email application. In this embodiment, the process (1100) comprises the steps of providing (1110) multiple spam detection schemes by an email application. Next, access to each spam detection scheme is provided (1120) from a single control window or graphical interface control.

[0061] FIG. 12 is a flowchart showing an embodiment of a method for visually representing a spam message according to a particular spam detection scheme. In this embodiment, the process (1200) comprises the step of providing (1210) multiple spam detection schemes or approaches. Further, the process comprises designating (1220) an email message as spam according to a particular detection scheme. The next

step includes marking (1230) the email message with a particular identifier of the particular detection scheme. Then, the identification of the email message with the particular identifier is displayed (1240) in a particular manner that is associated with the particular identifier. For example, an email message (or identification) that is associated with a particular identifier may be displayed in a certain font, style, color, *etc.* that is associated with the particular identifier. Accordingly, another identifier associated with another detection scheme may cause an email message (or identification) to be displayed in a different font, style, color, *etc.* Hence, the process (1200) may also include the step of recognizing (1250) which particular detection scheme designated the email message as spam based upon the visual representation or depiction of the email message.

[0062] FIG. 13 is a flowchart showing one embodiment, among others, of a method for detecting an undesired email message. In this embodiment, the process (1300) comprises several detection schemes that have been activated by the user or an administrator of the user's email settings and services. In other embodiments, however, a user or administrator may not have each of the detection schemes activated as shown or may have different types of spam detection schemes that are available to be activated.

[0063] In the embodiment shown in FIG. 13, the process (1300) comprises the step of determining (1310) the sender of an email message, as has been previously described. Preferably, identification of the sender is obtained from the header of the email message. If the identification of the sender provided from the email message matches (1320) a person's identification in the address book of a user, then an attempt is performed to verify (1330) the identification of the sender in the email message as the actual sender of the email message, as previously described. After the sender of the email message has been verified to be a person who is listed in the user's address book, the email message has been determined to not be spam (*e.g.*, an undesired email message) and is moved (1340) to the inbox of the user (or, in other embodiments, left to remain in the inbox). Alternatively, if the identification of the sender (from the email message) is not (1320) in the address book of the user or is not verified (1330) to be the actual sender, then the email message is further examined to determine if the email message is spam.

[0064] Accordingly, the email message is checked (1350) to determine if the content of the email message contains any words that have been determined to be objectionable by the user or an administrator (hereinafter, referred to as a text filter). If the email message is detected to contain undesirable words by the text filter (1350), the email message is

determined to be spam and is sent (1360) to a spam folder of the user or another designated user (such as a parent of a user). Alternatively, if the email message passes the text filter or is not detected to contain any undesired words by text filter, the process (1300) continues to allow the email message to be further examined by other spam detection schemes.

[0065] Correspondingly, the sender (as identified by the header of the email message) is checked (1370) against an allow list, as previously described, if the allow list detection mechanism has been activated (1365). Accordingly, if the sender is included on the allow list (1370), then the email message is determined to not be spam and is moved (1340) to the inbox of the user (or, in other embodiments, left to remain in the inbox). Alternatively, if the sender is not included on the allow list (1370), the email message is determined to be spam and the email message is sent or moved (1360) to the spam folder of the user or another designated user. Note, in the embodiment shown in FIG. 13, when the spam detection scheme of checking against an allow list is activated, then the spam detection scheme of checking against a block list is not performed. Accordingly, if the spam detection scheme of checking against an allow list is not activated (1365), then the step of checking against a block list is performed (1380). In other embodiments of the invention, checking against both an allow list and a block list may be enabled, checking against both an allow list and a block list may be enabled, in which case the allow list would not exclude email messages.

[0066] Next, the process (1300) continues by checking the sender of email message against a block list, in step 1380, as previously described. If the sender is included in the block list, the email message is determined to be spam and is moved (1360) to the spam folder of the user or another designated user. Alternatively, if the sender is not included (1380) in the block list, the email message is checked (1390) against a statistical filtering algorithm that is used to detect undesired email messages, as previously described. Correspondingly, if the statistical filtering algorithm determines (1390) the email message to be spam, then the email message is moved (1360) to the spam folder of the user or another designated user. Alternatively, if the statistical filtering algorithm determines (1390) the email message to not be spam and passes the email message, the email message is moved (1340) to the inbox of the user (or, in other embodiments, left to remain in the inbox).

[0067] Any process descriptions or blocks in flow charts should be understood as

representing modules, segments, or portions of code which include one or more executable instructions for implementing specific logical functions or steps in the process, and alternate implementations are included within the scope of the preferred embodiment of the present invention in which functions may be executed out of order from that shown or discussed, including substantially concurrently or in reverse order, depending on the functionality involved, as would be understood by those reasonably skilled in the art.

[0068] The email application 155 and mail store 220 may be implemented as a computer program, which comprises an ordered listing of executable instructions for implementing logical functions. As such the email application 155 can be embodied in any computer-readable medium for use by or in connection with an instruction execution system, apparatus, or device, such as a computer-based system, processor-containing system, or other system that can fetch the instructions from the instruction execution system, apparatus, or device and execute the instructions. In the context of this document, a "computer-readable medium" can be any means that can contain, store, communicate, propagate, or transport the program for use by or in connection with the instruction execution system, apparatus, or device. The computer-readable medium can be, for example but not limited to, an electronic, magnetic, optical, electromagnetic, infrared, or semiconductor system, apparatus, device, or propagation medium. More specific examples (a nonexhaustive list) of the computer-readable medium would include the following: an electrical connection (electronic) having one or more wires, a portable computer diskette (magnetic), a random access memory (RAM) (electronic), a read-only memory (ROM) (electronic), an erasable programmable read-only memory (EPROM or Flash memory) (electronic), an optical fiber (optical), and a portable compact disc read-only memory (CD-ROM) (optical). Note that the computer-readable medium could even be paper or another suitable medium upon which the program is printed, as the program can be electronically captured via, for instance, optical scanning of the paper or other medium, then compiled, interpreted or otherwise processed in a suitable manner if necessary, and then stored in a computer memory.

[0069] Although exemplary embodiments have been shown and described, it will be clear to those of ordinary skill in the art that a number of changes, modifications, or alterations to the invention as described may be made. All such changes, modifications, and alterations should therefore be seen as within the scope of the disclosure. It should be emphasized that the above-described embodiments of the present invention, particularly,

any "preferred" embodiments, are merely possible examples of implementations, merely set forth for a clear understanding of the principles of the disclosure. Many variations and modifications may be made to the above-described embodiments of the disclosure without departing substantially from the spirit and principles herein. All such modifications and variations are intended to be included herein within the scope of this disclosure.